INSTITUTO FEDERAL
SANTA CATARINA

CÂMPUS FLORIANÓPOLIS
DEPARTAMENTO ACADÊMICO DE SAÚDE E SERVIÇOS
CURSO SUPERIOR DE TECNOLOGIA EM GESTÃO DA TECNOLOGIA DA INFORMAÇÃO

ADEYVISON MOTA DE SOUSA

IMPLEMENTAÇÃO DA TÉCNICA DE PILHA DUPLA PARA TRANSIÇÃO DE REDES IPv4 PARA REDES IPv6

Florianópolis - SC
2018

Ficha de identificação da obra elaborada pelo autor

Mota de Sousa, Adeyvison
IMPLEMENTAÇÃO DA TÉCNICA DE PILHA DUPLA PARA TRANSIÇÃO DE REDES IPv4 PARA REDES IPv6 / Adeyvison Mota de Sousa ; orientação de Underléa Cabreira Corrêa; coorientação de Júlio Costa Ribas. - Florianópolis, SC, 2018.
66 p.

Trabalho de Conclusão de Curso (TCC) - Instituto Federal de Santa Catarina, Câmpus Florianópolis. CST em Gestão de TI. Departamento Acadêmico de Saúde e Serviços.
Inclui Referências.

1. Rede de Computadores. 2. IPv4. 3. IPv6. 4. Técnicas de Transição. I. Cabreira Corrêa, Underléa. II. Costa Ribas, Júlio. III. Instituto Federal de Santa Catarina. Departamento Acadêmico de Saúde e Serviços. IV. Título.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA
DEPARTAMENTO ACADÊMICO DE SAÚDE E SERVIÇOS
CURSO SUPERIOR DE TECNOLOGIA EM GESTÃO DA TECNOLOGIA DA INFORMAÇÃO

ADEYVISON MOTA DE SOUSA

IMPLEMENTAÇÃO DA TÉCNICA DE PILHA DUPLA PARA TRANSIÇÃO DE REDES IPv4 PARA REDES IPv6

Trabalho de Conclusão de Curso submetido ao Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina como parte dos requisitos para obtenção do título de Tecnólogo em Gestão da Tecnologia da Informação.

Professor Orientador:
Underléa Cabreira Corrêa, Profª Dra.

Professor Coorientador:
Júlio Costa Ribas, Profº Dr.

FLORIANÓPOLIS - SC
JUNHO / 2018

IMPLEMENTAÇÃO DA TÉCNICA DE PILHA DUPLA PARA TRANSIÇÃO DE REDES IPv4 PARA REDES IPv6

ADEYVISON MOTA DE SOUSA

Este trabalho foi julgado adequado para obtenção do Título de Tecnólogo em Gestão da Tecnologia da Informação e aprovado na sua forma final pela banca examinadora do Curso Superior de Tecnologia em Gestão da Tecnologia da Informação do Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina.

Florianópolis-SC, 18 de Junho de 2018.

_____
Felipe Cantorio Soares, Profº Msc.
Coordenador do CST em Gestão da Tecnologia da Informação
Instituto Federal de Santa Catarina

Banca Examinadora:

_____
Underléa Cabreira Corrêa, Profª Dra.
Orientadora
Instituto Federal de Santa Catarina

_____
Júlio Costa Ribas, Profº Dr.
Coorientador
Instituto Federal de Santa Catarina

_____
Adriano Heis, Profº Msc.
Instituto Federal de Santa Catarina

_____
Marcos Silvio da Rosa, Profº
Instituto Federal de Santa Catarina

À minha esposa, Carla, pela compreensão nos momentos difíceis.

AGRADECIMENTOS

Agradeço, inicialmente, ao Criador que me deu a oportunidade da vida e condições para poder aprender a cada dia e ser uma pessoa melhor. À minha esposa pela compreensão nos momentos de *stress* e pressões diversas do cotidiano. Sem seu apoio para seguir em frente, minha trilha até este momento seria muito mais difícil.

Agradeço à minha orientadora, que sempre indicou a direção correta para meus estudos, soube retirar o melhor de mim em termos de eficiência escrita, teórica, vislumbrando a melhor qualidade possível deste trabalho. Sou grato ao IFSC pelo tempo, profissionais e mestres oferecidos a mim, fornecendo os conhecimentos e motivações para almejar minha evolução como acadêmico e profissional da área.

“Vão em frente e peguem seus endereços IPv6!”

Latif Ladid, Fundandor e Presidente,
IPv6 Fórum.

RESUMO

Com a evolução que a tecnologia avança a necessidade de manter recursos para servir de base para essas tecnologias se tornam igualmente imprescindíveis. O IPv4, protocolo IP versão 4, que é responsável pelas comunicações entre computadores, e é a base da Internet que conhecemos, já atingiu a sua exaustão de oferta de IPs desde 2011. Antes desse fato ser concretizado o desenvolvimento de um novo protocolo IP fora especificado em meados da década de 1990. Com esses termos era criado o IPv6 com possibilidades de atendimento à humanidade por muitos e muitos anos, satisfazendo a necessidade de várias tecnologias que estão sendo desenhadas e implantadas na nossa sociedade. Este trabalho procurou definir um cenário básico para empresas migrarem suas infraestruturas de rede do padrão de Internet IPv4 para o IPv6. Foi desenhado um cenário controlado simulando uma empresa de pequeno porte a fim de verificar o fluxo de informações e o sucesso de conectividade no uso da Pilha Dupla ao acessar um servidor web remoto. Foram configuradas em todas as interfaces de rede os dois protocolos para ilustrar a Pilha Dupla, definindo um servidor DNS que resolveu o Nome de Domínio Completamente Qualificado (FQDN) e, de acordo com o algoritmo *Happy Eye Balls*, presente em conexões IPv6, retornou a página web em IPv6. O resultado do experimento foi o transito em IPv6, de acordo com o escopo proposto, que é quando há disponibilidade dos dois protocolos nas interfaces. A Pilha Dupla provou que é um método de transição viável da versão 4 do IP para a 6 e totalmente funcional.

Palavras-chave: Redes de Computadores, IPv4, IPv6, Técnicas de Transição.

ABSTRACT

With the evolution that technology advances the need to maintain resources to serve as a basis for these technologies also become indispensable. The IPv4 Internet Protocol version 4, which is responsible for communications between computers, and is the basis of the Internet as we know it, has already reached the exhaust your supply of IPs since 2011. Before that fact be completed the development of a new IP protocol out specified in the mid-1990. With these terms was created IPv6 with possibilities of service to humanity for many, many years, satisfying the need of various technologies that are being designed and implemented in our society. This work sought to define a basic scenario for companies to migrate their network infrastructures of the Internet IPv4 to IPv6. It was designed a controlled scenario simulating a small company to verify the flow of information and connectivity success in dual-stack usage when accessing a remote web server. Have been configured on all network interfaces both protocols to illustrate the Dual Stack, setting a DNS server solved the fully qualified domain name (FQDN) and, according to the algorithm Happy Eye Balls, present in IPv6 connections, return to web page in IPv6. The result of the experiment was the IPv6 traffic, according to the proposed scope, that is when there is availability of two protocols on the interfaces. The Dual Stack has proven that it is a viable transition method of version 4 of the IP for 6 and fully functional.

Key-words: Computers Networks, IPv4, IPv6, Transition Techniques.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

A (DNS)	*Hostname*, é o registro central de um DNS, ele vincula um domínio ou subdomínio a um endereço IPv4 direto.
AAAA (DNS)	Executam a mesma função de A, porém, para um endereço IPv6.
ARPANET	*Advanced Research Projects Agency Network*
CEPTRO	Centro de Estudos e Pesquisas em Tecnologia de Redes e Operações
CGNAT	*Carrier Grade NAT*
DHCP	*Dynamic Host Configuration Protocol*
DHCPv6	*Dynamic Host Configuration Protocol for IPv6*
DNS	*Domain Name System*
EUI-64	*Extended Unique Identifier*
FNUAP	Fundo de População das Nações Unidas
FQDN	*Fully Qualified Domain Name*
HD	*Hard Disk*
HOST-ID	Igual a endereço MAC
IANA	*Internet Assigned Numbers Authority*
ICMPv6	*Internet Control Message Protocol Version 6*
IETF	*Internet Engineering Task Force*
IoT	*Internet of Things*
IP	*Internet Protocol*
IPng	*Internet Protocol New Generation*
IPv4	*Internet Protocol versão 4*
IPv6	*Internet Protocol versão 6*
IS IS	*Intermediate System to Intermediate System*
ISO	*International Organization for Standardization*
ISP	*Internet Service Provider*
LAN	*Local Area Network*
LACNIC	Registro de Endereços da Internet para a América Latina e o Caribe
Log	Registro de eventos em um sistema de computadores
MAC	*Media Access Control*
MS-DOS	*Microsoft Disk Operating System*
NAT	*Network Address Translation*
NAT444	Igual a *Carrier Grade NAT*
NCP	*Network Control Protocol*
NETACAD	*Cisco Networking Academy*
NIC.br	Núcleo de Informação e Coordenação do Ponto BR
NTP	*Network Time Protocol*
OSI	*Open System Interconnection*

Ping	*Packet Internet Grouper*
PSP	*Peer to Peer*
QoS	*Quality of Service*
RAM	*Random Access Memory*
RFC	*Request for Comments*
RIP	*Routing Information Protocol*
RIPng	*Routing Information Protocol New Generation*
SLAAC	*Stateless Address Autoconfiguration*,
SO	Sistema Operacional
TCP/IP	*Transmission Control Protocol* e *Internet Protocol*
TFTP	*Trivial File Transfer Protocol*
TI	Tecnologia da Informação
Tracert	*Trace Route*
Túnel GRE	Túnel *Generic Routing Encapsulation*
VLAN	*Virtual Local Area Network*
VoIP	*Voice over IP*
VPN	*Virtual Private Network*
WEB	*World Wide Web*

SUMÁRIO

1. INTRODUÇÃO

A Internet, neste momento, faz parte da vida de todos. Atinge direta e indiretamente a vida do ser humano. Está presente em todas as aplicações financeiras, governamentais, informações, mídia e é base para várias interações entre as sociedades do planeta.

Historicamente é utilizada desde a década de 1960 e tinha como objetivo, dispor de um conjunto de comunicação militar, conhecida naquela época como ARPANET, que conectava grandes centros de pesquisa de universidades americanas e era financiada pela iniciativa militar. A rede tinha crescido tanto que o seu protocolo de comutação de pacotes original, chamado de *Network Control Protocol* (NCP), tornou-se inadequado. Deste modo, em 1981 surge a especificação da versão 4 do Protocolo da Internet, conhecida como IPv4 - *Internet Protocol* versão 4 (DUMAS, 2017).

Essa versão trabalha com endereços de 4 bytes (32 bits), possibilitando uma quantidade máxima de 2^{32} endereços, o que equivale a 4.294.967.296 endereços IPs (4 bilhões de IPs). Para os anos 80, essa quantidade de endereços, parecia suficiente. O modelo de negócio e as limitações tecnológicas quanto a mobilidade e comunicação sem fio, ainda estavam em desenvolvimento.

No entanto, no último trimestre de 2011, a população mundial alcançou a marca de 7 bilhões de pessoas. As tecnologias nano, sem fio e móveis atingiram seu pleno desenvolvimento, tornando a comunicação ubíqua uma realidade. As pessoas possuem computadores de mesa, de colo, de mão, computadores bibliotecas, TVs, e com mais frequência comprarão suas geladeiras, cafeteiras, e qualquer objeto que seja conveniente estabelecer comunicação.

O IPV4 não foi projetado para esse novo modelo da Internet. O que implica dizer que, atingiu novamente seu limite. Hoje temos a necessidade de cerca de um endereço IP para cada duas pessoas no planeta. Assim, a versão IPv6 surge com o objetivo de atender

esse novo contexto e dimensão da Internet, e traz implicações para todos os atuais e futuros negócios envolvidos com esse sistema.

Existem dois principais problemas do IPv4 hoje. O primeiro se relaciona ao limite do crescimento da Internet. No entanto, atinge principalmente, os novos negócios. Que obrigatoriamente deverão utilizar a versão 6 do IP. O segundo se relaciona aos negócios atuais, isto é, aqueles que fazem parte da atual arquitetura da Internet, a versão 4, e diz respeito a incompatibilidade da versão 6 do IP com a versão 4. O IPv6 foi estruturado sobre um outro formato que impede a coexistência da Internet IPv4. **Isso implica dizer que as redes IPv4 não conseguem acessar conteúdo da rede IPv6.**

Este trabalho busca estudar a nova versão do *Internet Protocol*, a versão 6 ou IPv6 e sugerir possíveis soluções na implantação / migração nas redes predominantemente IPv4 a fim de garantir o pleno funcionamento da Internet para as próximas gerações.

1.1. Justificativa

Atualmente a Internet passa por uma grande mudança tecnológica. Não há mais IPs livres para continuar se expandindo e para novo ingresso de usuários. O processo de transição da versão do IPv4 para a versão do IPv6 já começou. Os prazos para migração já estão encerrando e muitas empresas não iniciaram um plano de migração.

Com o atual cenário da indústria de informática, uma infinidade de dispositivos estão se conectando à Internet. Televisores, automação residencial, automóveis são alguns dos exemplos de integrantes de uma nova onda: a IoT (*Internet of Things*), Internet das Coisas. Sabe-se que dado a escassez de endereços versão 4 na atualidade e tendo em vista a iminente associação de bilhões de dispositivos na Internet, não há saída sustentável com o protocolo que temos (IPv4) e a solução definitiva para negócios que nasceram na versão

4 do IP é a adoção do novo protocolo IPv6. Considerando a incompatibilidade entre as versões de IP, as empresas precisarão realizar um processo de transição.

Assim, a importância do desenvolvimento deste trabalho de pesquisa se justifica pela dificuldade que muitas empresas encontram em adotar a nova versão do IP para sua infraestrutura de redes. Espera-se que com esse trabalho se possa oferecer uma estratégia básica que direcione e facilite o plano de migração entre os padrões de IP.

1.2. Definição do Problema

Em tempo de escassez de endereços IPv4, a problemática atinge empresas e pessoas por várias frentes.

A falta de endereçamento IP para novos negócios é um problema. Sem mais blocos de endereços para distribuir, os Provedor de Serviços de Internet (ISPs *Internet Service Provider*) não possuem mais *pool* de IPs para crescimento da Internet. Fato esse que impacta no crescimento da economia, pois novos sítios e soluções são inviabilizados. Novos negócios são dificultados e se precisarem de uma grande infraestrutura terão de ser realizados em outras regiões movimentando outros mercados. Não obstante esse problema, soluções paliativas e que comprometem a segurança da rede são desenvolvidas como uma sobrevida ao ciclo de vida do IPv4, como por exemplo o CGNAT (*Carrier Grade NAT ou NAT444)*, que compartilha IPs com milhares de usuários da Internet via provedor de acesso. Com esse tipo tradução são quebradas as conectividades de fim a fim como os jogos online, vídeo conferências, VoIP[1], etc.

Atinge inclusive o crescimento de empresas e sites já registrados. Um exemplo prático dessa problemática é uma empresa abrir filiais e precisar de serviços de acesso à

[1] Voice over IP ou Voz sobre IP - termo usado para a telefonia por IP. Inclui a configuração e transmissão de áudio digitalizado. (COMER, 2007)

Internet com IP fixo para comunicação e rotinas produtivas. Se não houver disponibilidade de novos IPs, como se dará o crescimento desta empresa?

O Centro de Estudos e Pesquisas em Tecnologias de Redes e Operações (CEPTRO) afirma que é utilizado por muitos provedores de Internet no Brasil o novo protocolo IPv6. Serviços como Facebook, Netflix e Google já possuem disponibilidade de tráfego utilizando esta tecnologia. Ainda de acordo com esta entidade, este tráfego representa 2% dos usuários conectados no Brasil.

A adoção do novo protocolo evolui a experiência de uso da Internet. Isso porque o IPv6 corrige falhas de segurança do IPv4 e resolve problemas de esgotamento de endereços IPs.

Segundo Santos (2009 pág. 40), a adoção do IPv6 pode permitir o surgimento de novas redes, irá aumentar o processo de inclusão digital, facilitar o surgimento de novas aplicações, evitar a utilização de técnicas como a NAT. No entanto, as empresas que possuem sua infraestrutura de rede sobre a versão 4 do IP, não será capaz de oferecer conectividade com a Internet versão 6, devido a incompatibilidade entre as mesmas. Provedores e empresas podem oferecer novos produtos aos seus clientes utilizando a nova tecnologia. O processo de transição já se iniciou, mas muitas empresas ainda não sabem como começar ou não estabelecem prioridades e ações para essa migração. Deste modo, nossa pergunta de pesquisa é:

"**O que as empresas que utilizam o padrão IPv4 devem fazer para transitar para o novo padrão de IPv6?**"

1.3. Objetivos

Para o desenvolvimento deste trabalho foram definidos os seguintes objetivos: geral e específicos.

1.3.1. Objetivo Geral

Definir e experimentar um cenário básico para as empresas migrarem suas infraestruturas de redes do padrão de Internet IPv4 para o padrão IPv6.

1.3.2. Objetivos Específicos

Para realização deste trabalho serão necessários os seguintes objetivos específicos:

- estudar as bases conceituais do IPv4 e IPv6;
- analisar os principais tipos de mecanismos, técnicas e estratégias de transição do IPv4 para o IPv6;
- criar um cenário que apontem estratégias de migração e implantação do IPv6 que atinja satisfatoriamente os requisitos para se ter uma conectividade do IP versão 6 com a Internet de forma a utilizar a versão 4 do IP, coexistindo no ambiente de produção;
- testar o cenário proposto utilizando um ambiente de simulação de uma empresa que ofereça e utilize serviços de Internet.

1.4. Estrutura do Trabalho

Este trabalho está estruturado em sete capítulos.

No primeiro capítulo estão estruturados o contexto que envolve o tema do trabalho, como também a definição do problema, objetivos gerais e específicos.

No segundo capítulo, na revisão da literatura se dá o embasamento teórico para o entendimento dos protocolos IPv4 e IPv6. Ainda neste capítulo são apresentados os conceitos dos principais métodos de transição para o IPv6.

No terceiro capitulo são apresentados os procedimentos metodológicos onde são ilustradas as etapas de execução deste trabalho.

Na sequência é definida a estratégia básica para a migração e implementação do IPv6 recomendando algumas práticas em relação a preparação para a migração para o novo protocolo IP.

No quinto capítulo é descrito o escopo do experimento tal qual o funcionamento deste e seus elementos. Ainda neste é apresentado o algoritmo *Happy Eye Balls* que possui fundamental importância na técnica da Pilha Dupla.

No capítulo seguinte são colhidos os resultados do experimento descrevendo as saídas que os sistemas operacionais apresentaram para os comandos executados.

Por fim, no último capítulo são apresentadas as considerações finais inerentes ao trabalho proposto. Também foram feitas as considerações acerca dos objetivos específicos e, ainda neste capítulo, foi sugerido uma área a explorar para trabalhos futuros.

2. REVISÃO DA LITERATURA

Estima-se que, segundo Francisco (2018) com dados do Fundo de População das Nações Unidas (FNUAP) em 2013, havia 7,2 bilhões[2] de pessoas no planeta e apresentando crescimento populacional cada ano, espera-se que em 2050 seremos 9 bilhões de pessoas Com uma parcela cada mês maior de usuários de sistemas com base na Internet a esmagadora maioria trafega na rede mundial utilizando o IPv4. A primeira vista pode parecer que toda rede funciona na sua normalidade, com os *hosts* conectados e trocando dados.

As redes IPv4 de hoje funcionam a custo computacional e financeiro relativamente altos. Isso porque são utilizadas técnicas de tradução de endereços IP para suprir a falta de endereços na rede, é o caso do NAT444 que foi idealizada como técnica de transição e, segundo o NICBR (Núcleo de Informação e Coordenação do Ponto BR), foi necessário para conservar os endereços IPv4, mas tem como fragilidade a quebra o modelo de comunicação fim a fim da Internet, ou seja, os dispositivos não podem ser alcançados diretamente, afetando o princípio da conectividade fim a fim da rede.

Em fevereiro de 2011 a IANA declarou oficialmente que o seu *pool* gratuito IPv4 se esgotou. Mudanças são necessárias, no entanto, muitas empresas procrastinam esse movimento por diversos motivos, dentre esses destacam-se:

- a demanda do setor de TI para configurar todos os hosts da empresa não apresenta contrapartida imediata que compense as horas de trabalho da equipe, na visão de muitos administradores;
- a infraestrutura deve estar atualizada para os ativos de rede poderem trafegar o novo protocolo. Atualizações de *firmware* nem sempre são o bastante para rodar o IPv6. Equipamentos eventualmente terão de ser adquiridos;

[2] Fonte: http://www.worldometers.info/br/ Acesso em 30 de março de 2017.

- provedores de acesso adotam como alternativa ao problema de falta de IP, algumas técnicas de transição tais como o CGNAT (Carrier Grade NAT) que por meio de compartilhamento de IP Público. Essa técnica satisfaz de maneira imediata e sem custos para as empresas, o problema de conectividade, sem considerar a transição para o novo protocolo. A inconveniência desta solução é a quebra do modelo de comunicação fim a fim da Internet pois os endereços públicos para os usuários são dinâmicos, o que abre uma lacuna de segurança. Atualizações como mapeamento de portas são implementadas mas não são soluções sustentáveis.

Para entender o problema, é necessário conhecer o protocolo IP, e o que muda entre a versão 4 e 6 deste protocolo.

Tanenbaum e Wetherall (2011, p. 25) definem protocolo como “um conjunto de regras que controla o formato e o significado dos pacotes ou mensagens que são trocadas pelas entidades pares contidas em uma camada.”

Assim como na comunicação humana de envio de uma carta simples, por exemplo (onde se encontra a identificação destinatário e do remetente, uma saudação, um conteúdo da mensagem, uma frase de encerramento), diversos protocolos têm de ser capazes de trabalhar conjuntamente para a comunicação entre *hosts* acontecer. E um grupo de protocolos que se inter-relacionam para desempenhar uma função de comunicação de dados é chamada de conjunto de aplicações de protocolos. Estes conjuntos são utilizados por *hosts* da rede.

Uma forma de visualizar esses conjuntos de protocolos é em formato de pilha. A *International Organization for Standardization* (ISO) é uma organização que normatiza os padrões técnicos de empresas e produtos e definiu um dos modelos existentes, que se chamou *Open Systems Interconnection* (OSI) *Reference Model*, em português, Modelo

OSI. Este possui sete camadas (veja Figura 1): 1- Física; 2 - Enlace; 3 - Rede, 4 - Transporte; 5 - Sessão; 6 - Apresentação e 7 - Aplicação.

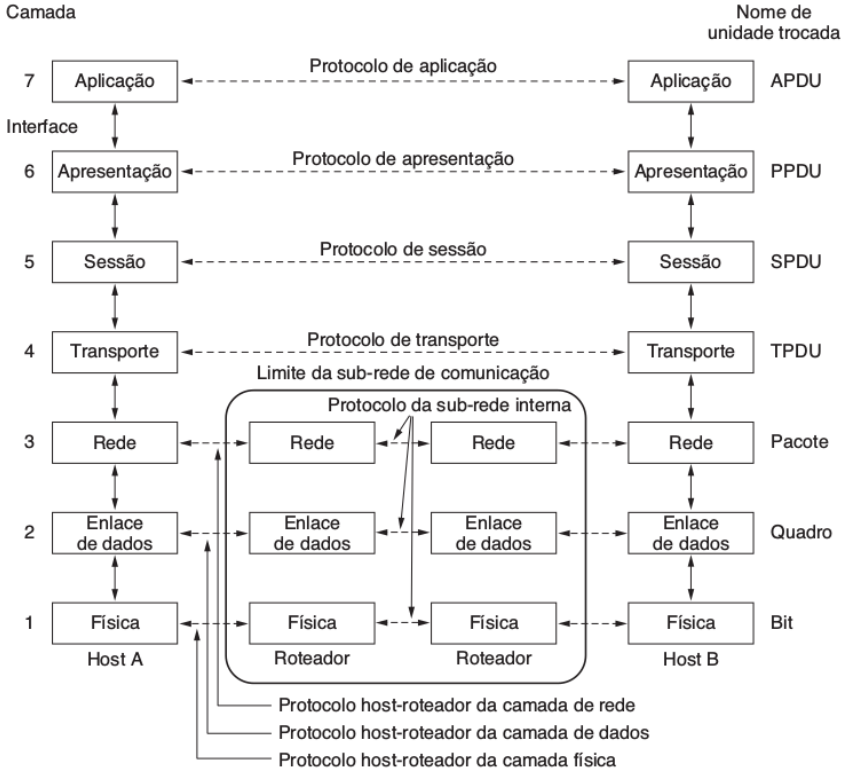

Figura 1: Modelo OSI.
(Fonte: Tanembaum, Wetherall (2011, p. 26))

Segundo o NetAcad Cisco (2014), uma pilha de protocolos mostra como os protocolos individuais dentro de um conjunto são implementados (veja Figura 2 das pilhas OSI e TCP/IP). Os protocolos são visualizados em camadas, com cada serviço de nível superior, dependendo da funcionalidade definida pelos protocolos mostrados nos níveis inferiores.

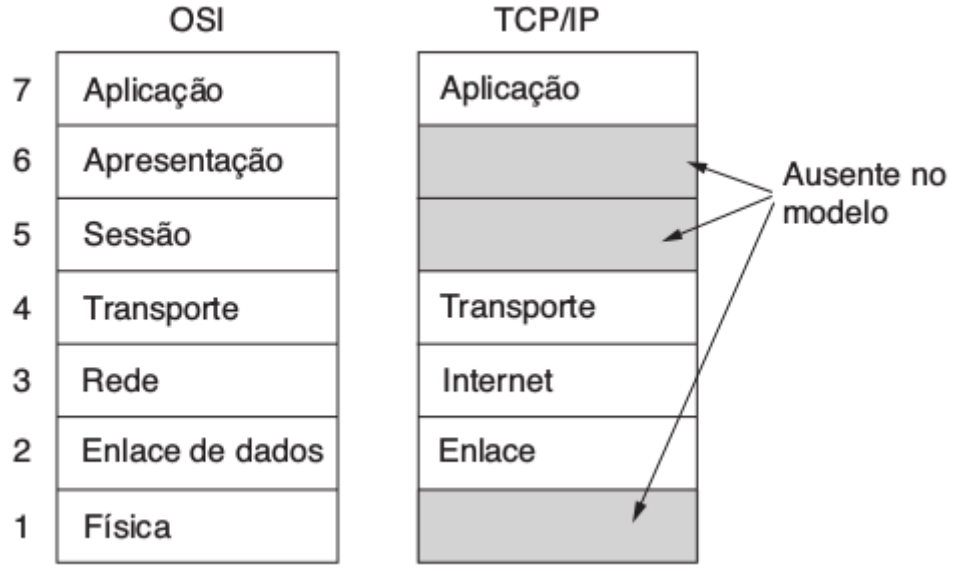

Figura 2: Modelo Referência OSI e TCP/IP.
(Fonte: Tanembaum, Wetherall (2011, p. 28))

Alguns autores como Tanembaum e Wetherall costumam utilizar um modelo híbrido, que é composto por cinco camadas, conforme mostra a Figura 3. Neste caso tem-se 5 camadas: 1- Física; 2- Enlace; 3- Rede, 4- Transporte, 5- Aplicação.

Figura 3: Modelo Híbrido
(Fonte: Tanenbaum, Wetherall (2011, p. 30))

2.1. O protocolo IP versão 4

O IP é o serviço da camada de rede implementado pelo conjunto de protocolos do Modelo TCP/IP (2014, NetAcad Cisco). Esse protocolo foi originalmente projetado para ter baixa sobrecarga, seu papel é apenas fornecer as condições necessárias para enviar um

pacote de uma origem a um destino por um sistema de redes interconectadas. As características básicas do IP são:

- **sem conexão** - Nenhuma conexão com o destino é estabelecida antes de encaminhar os pacotes de dados;
- **melhor esforço (não confiável)** - A entrega do pacote não é garantida;
- **independente de meio físico** - A operação é independente do meio físico que transporta os dados.

Segundo Tanenbaum e Wetheral (2011, p. 277), um recurso que define o IPv4 são seus endereços de 32 bits. Cada equipamento de usuário e de rede, como roteadores Internet possuem um endereço IP que é usado nos campos Endereço de origem e Endereço de destino dos pacotes IP, conforme mostrado na Figura 4.

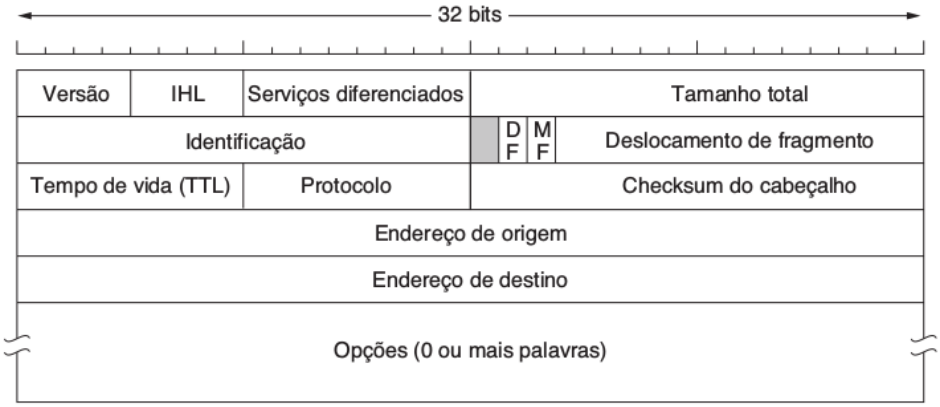

Figura 4: O cabeçalho IPv4
(Fonte: Tanenbaum, Wetherall (2011, p. 275))

De acordo com Comer (1998, p. 7), o que faz com que a tecnologia TCP/IP seja tão notável deve-se, em parte, a sua utilização quase que universal, e também à dimensão e à taxa de crescimento da Internet. A maioria esmagadora do tráfego corrente na Internet é baseado sobre o protocolo IPv4.

Um endereço IPv4 é composto por 32 bits. esses bits são segmentados em 4 campos de 8 bits que são expressados em formato decimal, de 0 a 255, separados por ponto final (“.”).

Exemplo:

11000000.10101000.00000011.00011000 = 192.168.3.24

No seu projeto inicial, que não sofreu mudanças até hoje, a quantidade de endereços possíveis eram de 2^{32} ou mais de 4,3 bilhões de endereços. O grupo IPV6.BR (2012) afirma que apesar do seu sucesso e robustez, facilidade de implantação e interoperabilidade, com o passar dos anos não pode prever alguns pormenores, tais como:

- crescimento dos hosts conectados e escassez de endereços IP;
- aumento das tabelas de roteamento;
- problemas ligados a segurança de pacotes transmitidos;
- segurança na entrega de determinados pacotes.

Como citado no início deste trabalho, as novas tecnologias e o aumento da demanda por endereços IPs culminaram no desenvolvimento de um protocolo mais atual e pronto para o devido uso, o *Internet Protocol* versão 6.

2.2. O protocolo IP versão 6

Na década de 1990 as autoridades da Internet já percebiam a iminente exaustão do protocolo IPv4 e em dezembro de 1993 a IETF através da RFC 1550 formalizou o pedido para pesquisa do novo protocolo IP, tido na ocasião sendo chamado por (*Internet Protocol Next Generation* (IPng).

As principais questões que deveriam ser levadas em consideração para o novo protocolo eram:

- **escalabilidade**: a rede deveria ter suporte para crescimento futuro, com novos usuários, hosts e redes conectadas;

- **segurança:** o novo protocolo deveria prover mais recursos de segurança, haja visto que pragas virtuais já prejudicavam a rede na época;
- **configuração e administração de rede:** teria de ser altamente configurável para a administração global da rede;
- **suporte a QoS:** deveria fornecer o serviço nativamente, abrindo caminho para tráfego intenso como VoIP;
- **mobilidade:** deveria solucionar questões de trânsito de hosts em diferentes redes, sem perder suas características,
- **políticas de roteamento:** evolução no contexto de roteamento;
- **transição:** deveria possuir métodos que facilitassem a transição do antigo protocolo para o novo.

Dentre as características acima mencionadas, a transição é o foco deste trabalho de pesquisa e para tal serão estudadas técnicas de transição do IPv4 para o IPv6, adequadamente abordadas na Seção 5.2.1 deste capítulo.

Para compreender o IPv6 é preciso considerar o sistema numérico com base hexadecimal. Assim como o decimal é um sistema de numeração com base dez e o binário é base dois, hexadecimal é um sistema de representação numérica com base 16. Como os endereços IPv4 são expressados em notação decimal por pontos (ex: 192.168.2.0) e, diferentemente, a numeração hexadecimal usa valores de 0 a 9 e letras de A a F.

Segundo NetAcad Cisco (2014), há 16 combinações diferentes de 4 bits de 0000 a 1111. Nesse sistema de 16 dígitos hexadecimais os 4 bits podem ser representados por um único valor hexadecimal.

O IP versão 6 têm comprimento de 128 bits e são escritos com uma sequência de hexadecimais, ou seja, para cada dígito hexadecimal representados são necessários 4 bits totalizando 32 valores hexadecimais. Por exemplo:

2001:0DB8:AD1F:25E2:CADE:CAFE:F0CA:84C1

Segundo o grupo do NIC.BR (2012), existem no IPv6 três tipos de endereços definidos:

- **unicast** – este tipo de endereço identifica uma única interface, de modo que um pacote enviado a um endereço *unicast* é entregue a uma única interface;
- **anycast** – identifica um conjunto de interfaces. Um pacote encaminhado a um endereço *anycast* é entregue a interface pertencente a este conjunto mais próxima da origem (de acordo com distância medida pelos protocolos de roteamento). Um endereço anycast é utilizado em comunicações de um-para-um-de-muitos;
- **multicast** – também identifica um conjunto de interfaces, entretanto, um pacote enviado a um endereço *multicast* é entregue a todas as interfaces associadas a esse endereço. Um endereço *multicast* é utilizado em comunicações de um-para-muitos.

Para Comer (2006), foram agrupadas mudanças introduzidas pelo IPv6 em sete categorias:

- ***endereços maiores:*** o novo protocolo conta com 128 bits contra os 32 bits do IPv4;
- ***hierarquia de endereços estendida:*** usa espaço de endereço maior para criar níveis adicionais de hierarquia de endereçamento, para um ISP aloque blocos de endereços para um cliente, por exemplo;
- ***formato de cabeçalho flexível:*** uso de um datagrama totalmente novo que inclui um conjunto de cabeçalhos opcionais;
- ***opções avançadas:*** O IPv6 permite que um datagrama inclua informações de controle opcionais, não disponíveis no IPv4;
- ***provisão para extensão de protocolo:*** em vez de especificar todos os detalhes, a capacidade de extensão do IPv6 permite que o IETF adapte o protocolo ao novo hardware de rede e novas aplicações;

- ***suporte para autoconfiguração e renumeração:*** o IPv6 permite que os computadores em uma rede isolado atribuem endereços locais automaticamente; o projeto também permite que um gerente renumere redes em um site dinamicamente;
- ***suporte para alocação de recursos:*** O novo protocolo inclui uma abstração de fluxos e bits para a especificação de diferenciação de serviço (*Diff Serv*). O último é idêntico ao *Diff Serv* do IPv4.

2.3. Transição do IPv4 para o IPv6

Segundo a iniciativa IPv6.br, grupo de trabalho do NIC.BR, o período de transição e de coexistência entre os protocolos IPv6 e IPv4 exigiu o desenvolvimento de técnicas auxiliares, inicialmente para resolver problemas de como conectar as novas redes IPv6 com o conteúdo das demais redes majoritariamente IPv4. Assim novas técnicas e métodos foram e continuam sendo desenvolvidas.

O grupo IPv6.br (2012), descreve essas técnicas de transição que podem ser encaixadas nas seguintes categorias:

- **pilha dupla:** É a coexistência de nós IPv4 e IPv6 no mesmo dispositivo. É a técnica padrão para a transição e deve ser usada sempre que possível;
- **túneis:** Permitem que haja tráfego de dados IPv6 em redes IPv4 e vice-versa;
- **tradução:** Permitem que equipamentos IPv6 se comuniquem com outros IPv4 por meio de conversão de pacotes.

O grupo IPV6.BR ainda afirma que essas técnicas são subdivididas em *statefull* e *stateless*. Técnicas *statefull* são aquelas que necessitam de uso de software e tem alto custo financeiro e computacional porque é preciso manter tabelas de estado para processamento dos pacotes pela rede. Técnicas *stateless* não têm essa necessidade, os

pacotes são tratados de forma independente. A seguir são apresentados com mais detalhe as técnicas de transição.

2.3.1. Pilha Dupla: IPv4 e IPv6 em todos os dispositivos

O *Dual Stack*, termo em inglês da Pilha Dupla é a recomendação básica para a transição segura do IPv4 para o IPv6 (2012, IPV6.BR), tendo em vista que há muitos serviços e sítios que não estão disponíveis no novo protocolo.

É a configuração simultânea do IPv4 e IPv6 no mesmo dispositivo, assim não são necessários mecanismos de tradução. Quando um dispositivo utiliza o método dual stack a interface passa a se tornar híbrida trafegando os dois protocolos, conforme mostra a Figura 5.

Em alguns dispositivos já basta ativar o suporte para IPv6 e outros necessitam de uma atualização de *firmware* das interfaces de redes. Em geral os novos dispositivos já possuem suporte para o novo protocolo.

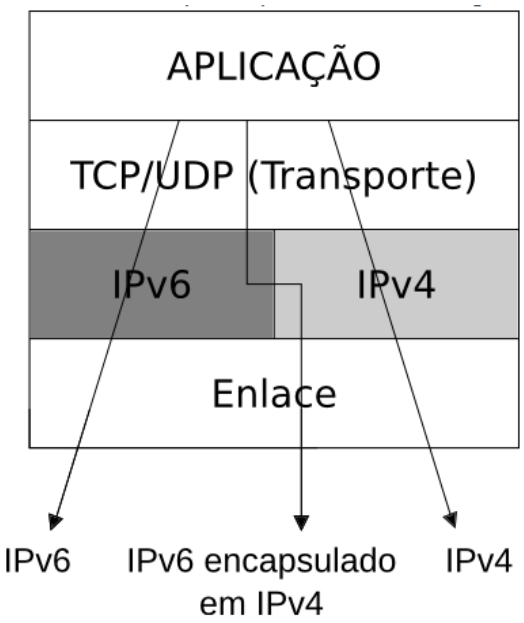

Figura 5: Funcionamento da Pilha Dupla.
(Fonte: ipv6.br/post/transicao)

2.3.2. Túneis

Túneis, também conhecidos como encapsulamento são mecanismos que servem para atravessar redes que não possuem suporte para o protocolo em uso. Desta forma os pacotes IPv6 podem atingir outro ponto de uma rede exclusivamente IPv4.

De acordo com o portal IPv6 do LACNIC[3] os pacotes são transportados até um ponto da rede em que ele é encapsulado e transmitido e ao atingir certo ponto o pacote é desencapsulado e encaminhado para a rede devida, na mesma versão do seu protocolo inicial.

Neste trabalho será apresentado os túneis 6over4, túneis GRE e Tunnel Broker

2.3.2.1 Túnel 6over4

Segundo Gomes (2012), o 6over4 é uma das técnicas de transição mais antigas para o IPv6. Trata-se de *relays* de pilha dupla espalhada de forma colaborativa pelas redes, fornecendo conectividade IPv6 nas duas extremidades do túnel (veja Figura 6).

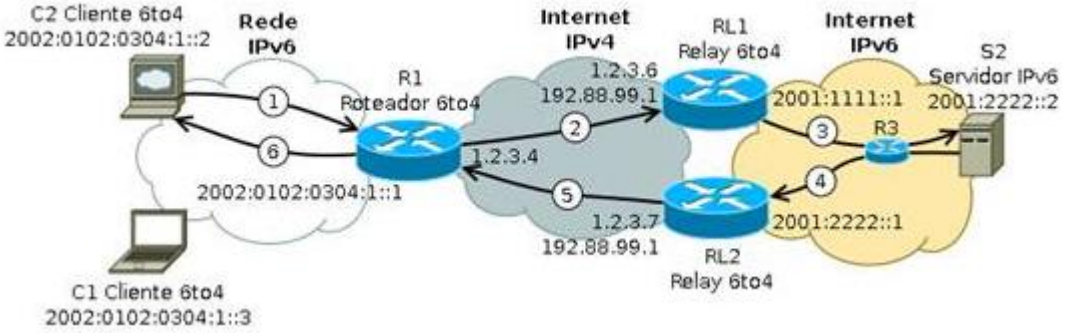

Figura 6: Tunnel 6over4

(Fonte: http://www.teleco.com.br/tutoriais/tutorialredeip2/pagina_3.asp)

[3] Registro de Endereçamento da Internet para a América Latina e o Caribe. É responsável pela designação e administração dos recursos de numeração da Internet (IPv4, IPv6), Números Autônomos e Resolução Inversa, entre outros recursos para a região da América Latina e o Caribe. É um dos cinco Registros Regionais da Internet no mundo. (LACNIC, 2017)

Esse tipo de túnel é estabelecido manualmente, de endereçamento estático. A criação desse túnel é relativamente fácil, tendo em vista que apenas se precisa fazer um cadastro em um sítio que é servidor de túneis e depois do serviço aprovado, fazer as configurações nas extremidades para se trafegar o IPv6.

2.3.2.2 Túneis GRE

É acrônimo do termo em inglês de *Generic Routing Encapsulation*, o Túnel GRE é outro tipo método de transição de configuração estática para trafegar dados IPv6 em redes IPv4 com a finalidade de encapsular pacotes IPv6, ISIS e outros (veja Figura 7), desenvolvido pela CISCO em parceria com a Juniper.

A configuração em Túnel GRE é manual. Essa característica faz do GRE um método não escalável e dependente de manutenção, sempre que algum parâmetro da rede mude. Este tipo de encapsulamento é suportado na maioria do sistemas operacionais e roteadores e possibilita a criação de um link ponto a ponto (ipv6.br, 2012). Foi desenvolvido para rodar vários protocolos, descritos na RFC 2784.

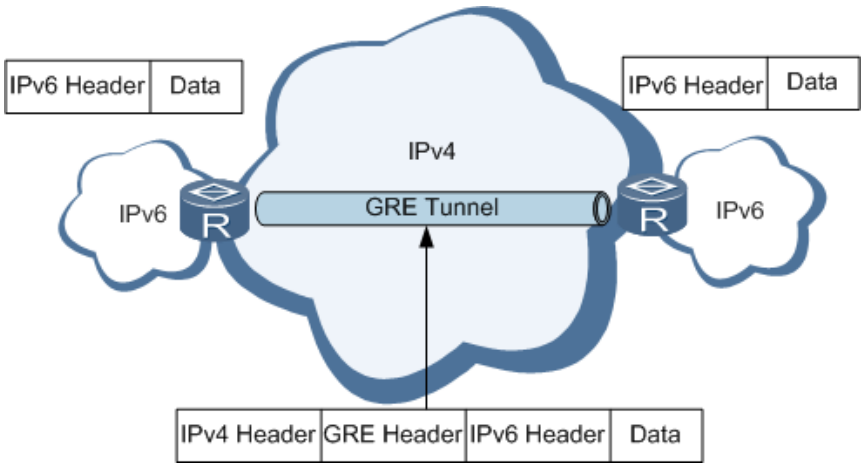

Figura 7: GRE Tunnel
Fonte: Huawei, 2017.

2.3.2.3 Tunell Broker

Segundo o grupo IPV6.BR (2012), trata-se de uma técnica que permite que dispositivos isolados ou uma rede inteira obtenha conectividade IPv6 graças a um túnel com um provedor especializado, chamado de *Tunnel Broker* e, a partir dessa conectividade, torna os dispositivos de pilha dupla (veja Figura 8). O *Broker* de forma automática ou semi-automaticamente configura IPv6 nos clientes por via de *script*, software ou instruções.

É recomendada para usuários domésticos ou pequenas empresas que querem se familiarizar com o IPv6, quando seus provedores de acesso não dão suporte para o novo protocolo IP.

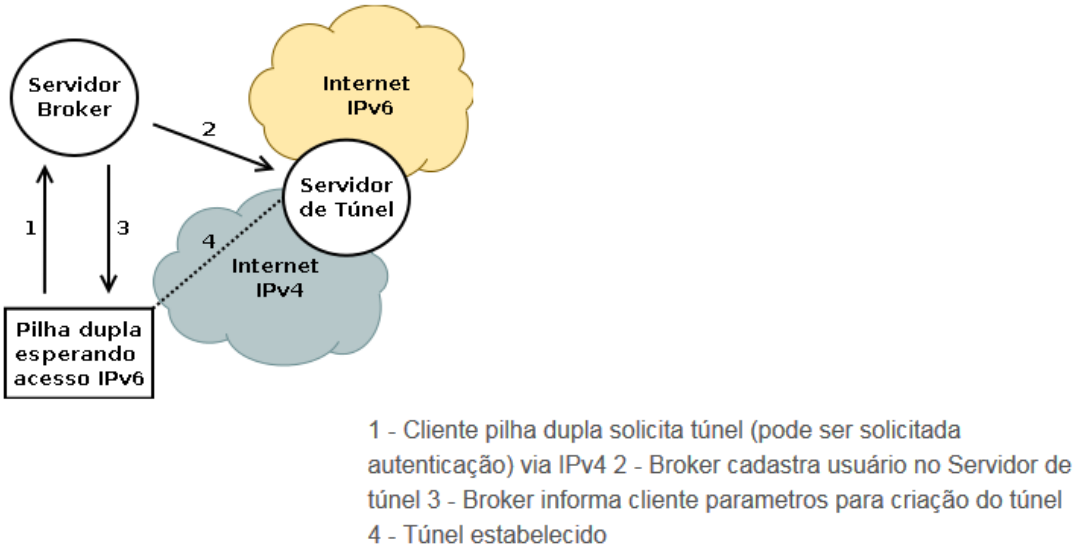

Figura 8: Topologia lógica do Tunnel Broker
(Fonte: IPV6.BR, 2012)

2.3.3. Tradução de Endereços IP

Considerando a escassez de endereços IPv4, a técnica de tradução de endereço privados em endereços públicos denominada NAT (*Network Address Translation*), com descrição na RFC 3022, foi uma das primeiras estratégias desenvolvidas para ampliar a utilização do IPv4. Inicialmente, surgiu o NAT. Uma empresa que possuía 100 *hosts*, por exemplo, antes da técnica precisaria de 100 IPs públicos para acessarem a rede. Após a

implementação deste recurso, os mesmos 100 endereços privados passam pelo roteador de borda da empresa e recebem um único endereço público.

Mas como descrito acima, mesmo utilizando o NAT para obter menor impacto nos IPs públicos, não foi suficiente para o uso com cautela do IPv4, tendo em vista a quantidade de novos IPs fazendo o *logon* na rede a cada dia. Como uma técnica de transição para um novo protocolo que viria, descrito na RFC 6264, surge o CGNAT ou NAT444, que é a tradução em grande escala de pacotes IPv4, feitas pelas provedoras de acesso à Internet.

2.3.3.1 NAT444 ou CGNAT

Segundo o grupo IPV6.BR (2012), o CGNAT tem sido usado no objetivo de prolongar a vida útil do IPv4. É um mecanismo que utiliza uma faixa de IP específica (RFC 6598) dentro da rede da ISP que os usuários são conectados e ao passar no roteador de borda da provedora, compartilha endereços IP públicos (veja figura 9).

O CGNAT foi desenvolvido para ser uma técnica auxiliar na transição para o IPv6. Foi muito importante para Internet para preservar os endereços IPv4. Segundo Kurose (2013), seu uso acompanha grandes restrições de puristas do IETF. Dentre essas a conectividade fim a fim da Internet não deve ser quebrada modificando IP ou porta de destino ou origem; roteadores só devem processar pacotes até a camada 3.

O uso no CGNAT não deve ser usado imprudentemente como forma de solução do problema de escassez de endereços IP versão 4. Conexões de VoIP, P2P[4], jogos e videoconferências se tornam inviáveis com essa tradução.

[4] P2P (do inglês peer-to-peer, que significa par-a-par) é um formato de rede de computadores em que a principal característica é descentralização das funções convencionais de rede, onde o computador de cada usuário conectado acaba por realizar funções de servidor e de cliente ao mesmo tempo. (Ciriaco, 2008).

É importante ressaltar que é uma técnica cara pois exige ativos de rede com alto poder de processamento. Custos com compras desses equipamentos tendem a dificultar novos investimentos para a adoção do IPv6.

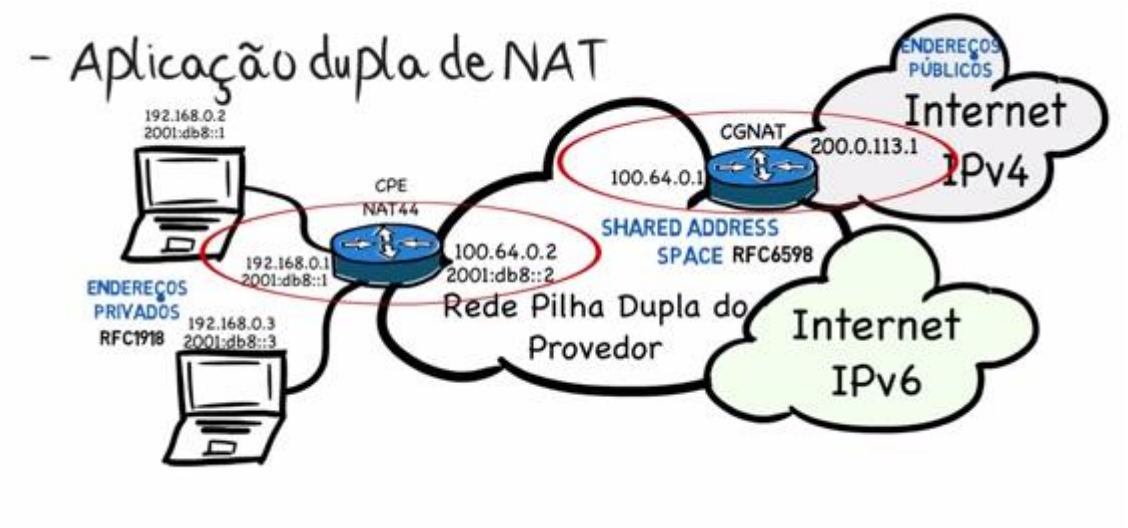

Figura 9:Diagrama do CGNAT (NIC.BR, 2014)

3. PROCEDIMENTOS METODOLÓGICOS

O presente trabalho tem natureza aplicada, com abordagem do problema de modo teórico e prático, assumindo o caráter de um estudo de caso experimental, a fim de criar e testar um cenário com alternativas básicas para as empresas iniciarem seu processo de migração para o IPV6. O trabalho foi desenvolvido em 4 etapas, dentre as quais estão: 1: Revisão do Referencial Teórico, 2: Diretrizes para Implementação do Experimento, 3 Experimento em Ambiente Virtual e 4: Conclusões, conforme ilustra a Figura 10.

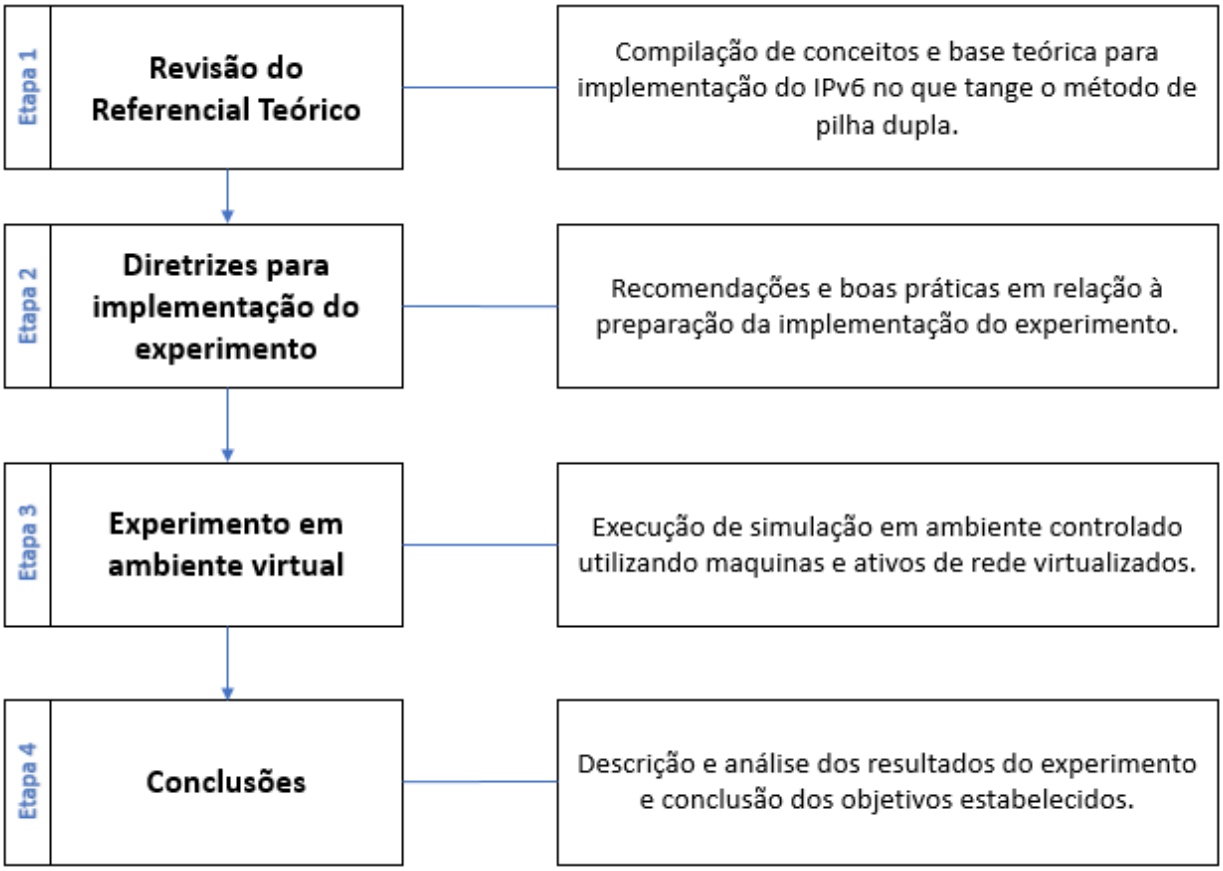

Figura 10: Etapas deste trabalho.

Para a fase de teste, optou-se pela descrição de uma empresa com característica de pequeno porte que servirá de base para o cenário experimental. Por fim são apresentados os resultados obtidos dentro deste cenário.

4. ESTRATÉGIA BÁSICA PARA A MIGRAÇÃO E IMPLEMENTAÇÃO DO IPV6

Nesta seção serão apresentadas recomendações básicas e boas práticas em relação a preparação para a primeira fase de migração para o IPv6.

Considerando um cenário onde a empresa precisa manter sua infraestrutura IPv4 por mais um tempo rodando, mas sem deixar de se conectar com a nova rede IPv6, a estratégia mais convenientemente indicada é o uso da **pilha dupla.**

4.1. Considerações básicas para a Pré-Implantação do IPv6

É preciso deixar claro que, para que esta técnica de transição se torne possível é indispensável que o *ISP* forneça no seu serviço de Internet a conectividade IPv6. A partir dessa necessidade satisfeita a técnica de Pilha Dupla pode ser possível no âmbito de implementação.

Acerca das considerações, estão relacionadas sobre a perspectiva ao que diz respeito a compatibilidade, planejamento e plano de endereçamento. As principais etapas são ilustradas de acordo com a figura 11.

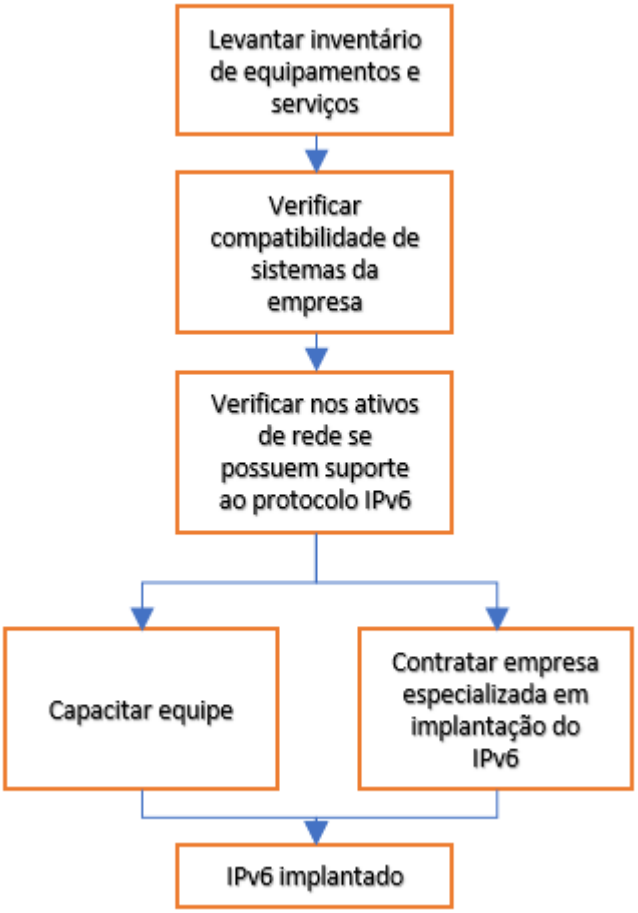

Figura 11:Etapas para implantação do IPv6.

De acordo com a figura 11, antes de começar a configurar os ativos de rede é altamente recomendável construir um inventário de equipamentos, serviços e softwares utilizados pela empresa atualmente. Verificar se sistemas de gestão têm compatibilidade com o novo protocolo é muito importante do ponto de continuidade do serviço.

O IPv4 continuará por muitas décadas, mesmo sendo utilizada como tecnologia legada. Mas frente à novas possibilidades de uso, otimização, segurança, é desejável ter o máximo possível de serviços físicos e lógicos rodando, preferencialmente em IPv6.

Saber se o parque de informática pode ter conectividade IPv6 é importante pois pode-se verificar a necessidade de troca de equipamentos com alguma obsolescência para versões mais modernas que podem trafegar ou processar os dados com mais agilidade.

Ter uma equipe engajada e capacitada para a implementação do IPv6 é de fundamental importância para o sucesso deste projeto. Alternativamente empresa poderá contratar uma capacitação para sua equipe de TI, ou uma empresa que execute o processo de transição.

4.2. Planejando a rede

Os dispositivos de rede devem possuir suporte ao IPv6, assim como os hosts, servidores e demais clientes que se conectam na rede do novo protocolo.

A **Pilha Dupla** deve ser utilizada devido ao contexto de transição. O uso da Pilha Dupla nas redes (NIC.BR, 2014), favorece a escalabilidade e o estabelecimento gradual do novo protocolo até ser aceitável e prudente desligar a rede IPv4.

Se houver conectividade IPv6 via ISP, no caso de empresas, deve-se ter um bloco de no mínimo /48 bits, que gera 65636 sub-redes. Se o provedor oferecer um prefixo menor, será necessário questionar. Um endereço de prefixo /64 é recomendado, de acordo com o NIC.BR, para clientes residenciais.

Além da configuração do IPv6 nas interfaces, muitas aplicações do tipo Banco de Dados, logs, etc., necessitarão de mudanças adicionais, por exemplo: resolução DNS precisará atender requisições A e AAAA, planos de endereçamento para cada protocolo IP, políticas de resolução de problemas diferentes, etc.

A maioria dos Sistemas Operacionais suportam o IPv6, mas existem algumas nuances que devem ser observadas e testadas fora do ambiente de produção. Em resumo, toda a Infraestrutura deve estar preparada para rodar, processar, encaminhar todos os dados que uma rede IPv4 é capaz de rodar. O gestor TI deverá verificar o nível de compatibilidade do SO utilizado na empresa com o IPv6.

4.3. Endereçamento

Para se planejar uma rede em pilha dupla se faz necessário ter um plano de endereçamento onde se formalizará os IPs dos servidores, *gateways*, demais dispositivos daquela rede, tal qual VLANs e dispositivos componentes das mesmas.

Caso a rede não tenha esse plano, como boa prática é interessante nomear os dispositivos, para uma resolução DNS dentro da LAN tanto quanto servidores, impressoras e dispositivos que fornecem serviços para a rede estejam com endereços IPs estáticos.

Para todos os outros hosts conectados na rede sugere-se definir um *pool* de IPs para utilização. Esse *pool* deve abranger os IPs que serão alugados para cada host e por quanto tempo deve ser cedido até ser liberado para outro *host* ou renovado. Esse serviço é executado pelo servidor DHCP (Dynamic Host Configuration Protocol) que é um protocolo definido para esse propósito.

No caso do IPv6 este protocolo se chama DHCPv6 e concede o endereço IPv6 de várias maneiras:

- **autoconfiguração *Stateless* (SLAAC):** que permite a aquisição de endereços globais sem o uso de DHCP;
- **configuração Estática:** modo de configuração manual de forma que o *host* tenha um endereço fixo, servidores em geral utilizam esse tipo de configuração;
- **configuração Estática EUI-64:** modalidade de configuração estática que automaticamente gera o sufixo identificador do *host* utilizando 48 bits do MAC da placa de rede e mais 16 bits de uma função de expansão específica para fornecer os 64 bits necessários para o sufixo;

- **DHCPv6 *Stateful*:** O servidor DHCPv6 mantém uma tabela com o estado dos clientes (endereço físico com os endereços lógicos atribuídos);
- **DHCPv6 *Stateless*:** modalidade onde o servidor DHCP utiliza as funcionalidades da autoconfiguração para fornecer apenas algumas informações como o endereço de um servidor DNS, ou NTP para algumas aplicações, TFTP, etc.

É preciso detalhar para fins de conhecimento de implementação os conceitos de SLAAC e DHCPv6. A escolha de um ou outro e até os dois combinados serão decisivos para uma aplicação justa, dentro da capacidade de processamento dos ativos de rede e necessidade de cada cenário.

4.3.1. SLAAC

A autoconfiguração é uma das características do IPv6. É possível se autoconfigurar toda uma rede de computadores sem a necessidade de ter um servidor DHCP. Essa forma de autoconfiguração se chama SLAAC (*Stateless Address Autoconfiguration*). Esse método não mantém nenhum registro do seu endereço atribuído (*stateless*) e é automaticamente atribuído nos *hosts* (*autoconfiguration*), daí a origem do seu nome (BRITO, 2013).

O processo de autoconfiguração de IPs versão 6 funcionam basicamente em duas etapas: **(i)** a configuração do prefixo do host, e **(ii)** a configuração do sufixo de host.

Na configuração do prefixo, os hosts aprendem seu prefixo de rede por meio de mensagens ICMPv6 do roteador. A segunda etapa, o sufixo, os últimos 64 bits são gerados a partir do endereço físico (MAC) da interface de rede adicionando uma função de expansão chamada EUI-64. Como o endereço físico possui 48 bits o EUI-64 adiciona os 16 bits restantes para integralizar o Host-ID de 64 bits.

O algoritmo EUI-64 funciona da seguinte maneira (veja Figura 12):

1. recebe o endereço 48 bits e separá-o em duas porções iguais;
2. adiciona os algarismos hexadecimais “FFFE” (16 bits) entre as duas porções;
3. inverte o 7º bit do primeiro *byte* para 1 (destacado em preto), indicando que o endereço é administrado localmente.

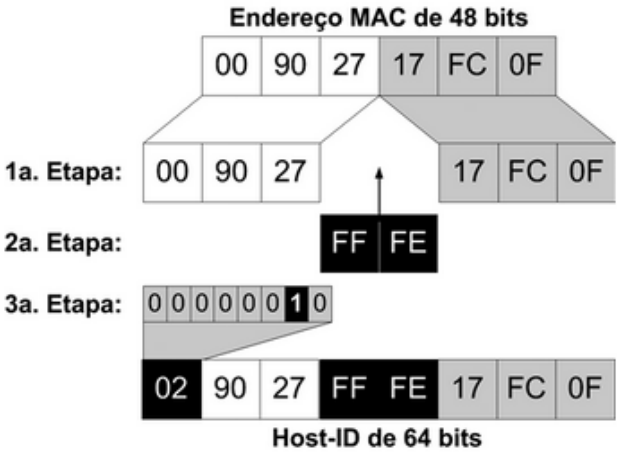

Figura 12: Aplicação da função EUI-64 na identificação do host.
Fonte: IPv6: Um novo protocolo. (Brito, 2017)

Após o algoritmo concluir os passos, as porções são unificadas para gerar um endereço global *unicast* automaticamente atribuído a interface que permite conexão no contexto local e da Internet.

Embora as empresas possam optar por atribuir o endereço por meio de outros mecanismos, o SLAAC será extremamente útil para facilitar o processo de atribuição de endereços na Internet das Coisas (BRITO, 2017).

4.3.2. DHCPv6

Assim como no IPv4 o DHCP para a versão 6 é um serviço de natureza *statefull* ou seja, registra os hosts em uma tabela, possui um *pool* de endereços, registra o *lease*, que é o tempo de aluguel de determinado IP para algum host.

Mas no IPv6 este protocolo pode ser implementado de forma *statefull* ou *stateless*. Pode ser implementado *stateless* funcionando com base no SLAAC e adicionalmente

apenas fornecendo o DNS a consultar e, ocasionalmente, serviços como TFTP ou NTP. Implementado de maneira *statefull*, se comporta como o DHCP versão 4, definindo um endereço dentro de uma faixa específica, o *lease* cedido. O escopo é explicitamente configurado. Pode ser implementado em Linux ou Windows como também em roteadores[5].

[5] Verificar a funcionalidade no roteador.

5. DESCRIÇÃO DO ESCOPO DO EXPERIMENTO

Esta seção apresenta o teste efetuado sobre a estratégia de migração entre o padrão IPv4 para o padrão IPv6 usando pilha dupla, no qual esse trabalho sugere. O teste foi efetuado sobre um cenário simulando uma empresa de pequeno porte a fim de verificar o fluxo de informações e o sucesso de conectividade no uso de Pilha Dupla ao acessar um servidor web remoto.

A empresa aqui definida possui um parque com uma rede interna e estação de trabalho utilizando o S.O. Windows 7 Profissional. As placas de rede são compatíveis com as duas versões do protocolo IP. A rede oferece os serviços de impressão em rede, acesso a servidor de arquivos interno e acesso à Internet. Em resumo, é uma rede de computadores com oferta de serviços básicos. Agrega-se maior complexidade nos ativos de rede, *hosts* e serviços à medida que o porte da empresa ou natureza do trabalho seja maior. O ponto de apoio para o experimento é qualquer tipo de empresa que se encaixe nesse modelo básico de conectividade com a Internet, seja ela deste porte ou com várias subredes, roteamentos entre filiais e serviços avançados de gestão e operação.

A topologia foi criada no software “GNS3”, que é um simulador gráfico de redes que emula ativos e topologias de rede. Possui ainda integração com máquinas virtuais e eventualmente a própria rede real que o host utiliza. Não obstante o software utilizado foram também utilizadas máquinas virtuais (vide figura 13) Windows 7, Windows Server 2008 R2 e imagens reais de roteadores Cisco, modelo C1700, imagem versão 12.4.

O objetivo principal desta topologia é fazer uma requisição ao servidor web a partir de um local remoto. Esta requisição antes de chegar no objetivo é resolvida no servidor DNS.

Considerando a inviabilidade de se conhecer o endereço IP de cada site que vamos acessar na Internet, pelo mundo estão espalhados milhares de servidores DNS (*Domain Name System*) que é o sistema de Nomes e Domínios. Simplificando ao máximo pode-se dizer que se trata de um servidor que possui uma tabela de IP´s e nomes de sites. Como resposta para o solicitante do site remoto este servidor retorna o IP para o navegador e assim continua-se a comunicação. Para este caso de estudo, em específico, foi configurado um servidor DNS na máquina virtual “W2008” com registro A e AAAA para a consulta do servidor web.

O servidor Web utilizado foi o APACHE, parte integrante *software* “XAMPP” versão 7.2.0 que provê servidor Apache, banco de dados “Maria DB” e interpretadores para linguagens de script PHP e Perl.

É importante dizer que os ativos estão configurados com pilha dupla. Pretende-se demonstrar a comunicação em IPv6 em redes com os dois protocolos ativados.

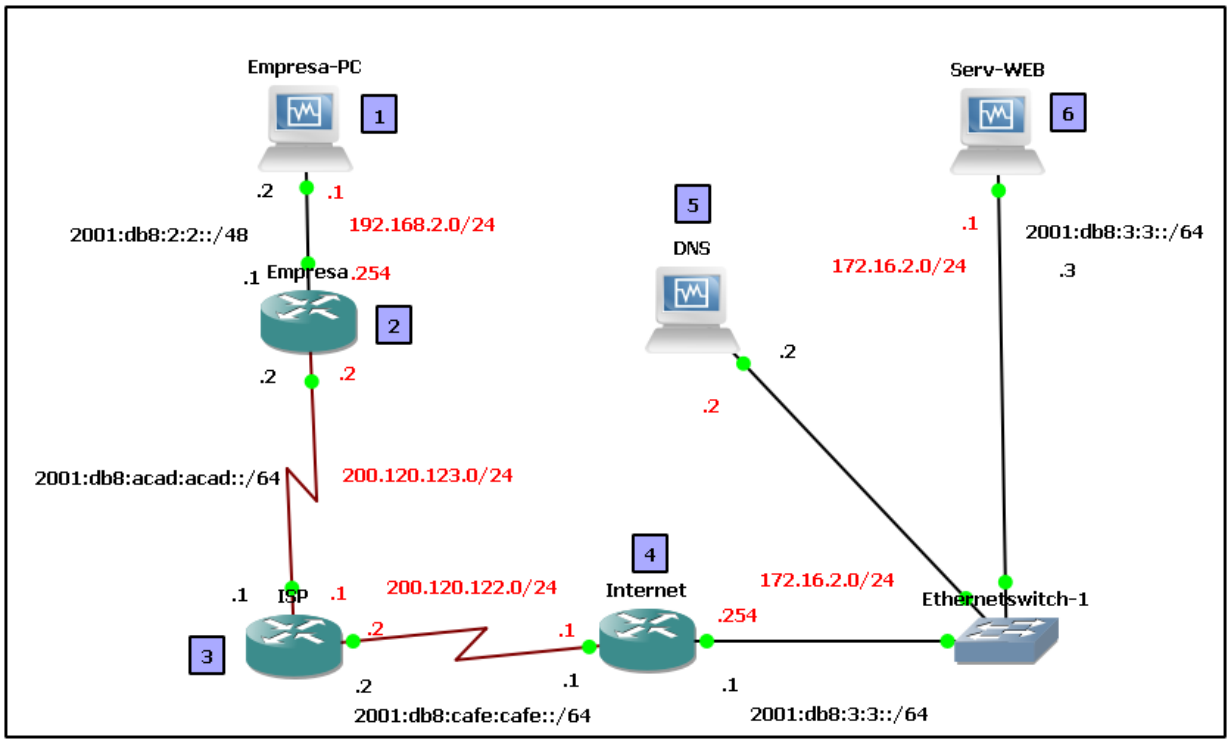

Figura 13: Topologia utilizada para o experimento.

De acordo com a Figura 13, para o ambiente de simulação foram implementadas em (1) uma máquina virtual, SO Microsoft Windows 7, 1GB de RAM, 20GB de HD representando um computador comum de alguma empresa, conectada em (2) um roteador Cisco, modelo C1700, imagem versão 12.4, representando o roteador da empresa, conectada em (3) roteador Cisco, modelo C1700, imagem versão 12.4, representando o roteador da operadora de Internet (ISP) conectado em (4) Cisco, modelo C1700, imagem versão 12.4, representando um roteador da Internet, conectado com (5) um comutador/switch genérico. Este comutador faz conexão com o servidor (6) DNS “W2008” e o computador remoto (7) uma máquina virtual, SO Microsoft Windows 7, 1GB de RAM, 20GB de HD, máquina essa que possui instalada o “XAMPP” e possui a página WEB a ser alcançada.

Para este experimento foram endereçadas todas as interfaces de rede estaticamente. Como boa prática é importante salientar que o endereçamento em uma LAN real deve ser feito de maneira automatizada, dentro do escopo definido pelo arquiteto da rede. Nessa realidade pode-se utilizar o DHCPv6 ou SLAAC como forma de endereçamento IPv6.

5.1. Happy Eyeballs

Para comprovar a eficiência da pilha dupla é preciso entender o *Happy Eyeballs*. Para um usuário que possui ambas conectividades, versão 4 e versão 6, a conexão acontecerá em apenas um protocolo.

O *Happy Eyeballs* é um método que tenta resolver o problema de decisão de conexão. Seu funcionamento consiste em tentar conectar os dois protocolos ao mesmo tempo e utilizar o que será estabelecido mais rapidamente dando uma leve preferência ao IPv6 (IPv6.br, 2012).

Simplificando ao máximo, no momento de acessar um domínio é verificado se há conectividade IPv4 e IPv6. Os sistemas operacionais e navegadores conectam primeiro no IPv6 e se houver *timeout* a conexão é descartada e os navegadores então, conectam-se em IPv4. Segundo o IPV6.br (2012), os navegadores Google Chrome e Mozilla Firefox em suas versões atuais já implementam o *Happy Eyeballs* e o utilizam por padrão.

Para os navegadores que não possuem essa função ativa por padrão ou percebe-se que por momentos a conexão acontece via IPv4 e noutro momento por IPv6, que é o caso do Safari da Apple, recomenda-se utilizar o Firefox Mozilla ou Chrome, referenciados na RFC 6555 como casos de sucesso na implantação do algoritmo. Adicionalmente, manter os navegadores e sistemas operacionais atualizados poderá, no futuro, resolver esse tipo de problema.

6. RESULTADOS DOS EXPERIMENTOS

Seguindo a topologia proposta, para a comunicação entre as diferentes redes simuladas foram configurados protocolos de roteamento dinâmico IPv6 com o RIPng e roteamento IPv4 utilizando o RIP em sua versão 2. Na Figura 13 demonstra o endereçamento na máquina empresarial de onde partirão as requisições.

Na simulação foi acessado o *prompt* de comando do Windows 7 na máquina “1” para o acesso a informações referente ao experimento. Em poucas linhas, o *prompt* de comando é uma interface não gráfica que oferece um ponto de entrada para a digitação de comandos do MS-DOS.

Ilustrado na Figura 14 está o comando “ipconfig” é um comando que retorna para o usuário informações acerca do protocolo IP da rede local. O objetivo na invocação deste comando foi confirmar os endereços IP versão 4 e 6 configurados na interface de rede. Adicionalmente o endereço do roteador da rede (*gateway*) foi informado. Este apontamento é fundamental para a comunicação com outra rede, trabalho que o roteador executa encaminhando pacotes IP a partir de sua tabela de roteamento.

Figura 14: Comando “ipconfig” para demonstrar a Pilha Dupla configurada.

Baseado na tabela de endereçamento desta simulação (anexo 1), foi executado um teste de conectividade à uma rede remota. Para efeitos de experimento, munido do endereço IPv6 do servidor WEB, ainda no *prompt* de comando, foi disparado o comando “ping 2001:db8:3:3::3”(vide Figura 15), a fim de alcançar este servidor e confirmar as configurações de roteamento RIPng nas 5 redes diferentes.

O comando “ping” é o acrônimo de *Packet Internet Network Groper* que é um sistema presente em praticamente todas as redes e sistemas operacionais e tem como finalidade mandar um conjunto de dados para uma máquina conectada e calcula o tempo em que essa mensagem retorna para a origem.

Na simulação, após dado o comando “ipconfig” foram obtidas respostas do servidor remoto confirmando que se encontra alcançável e *online*.

Ainda na Figura 15, são demonstrados os saltos até o servidor web, utilizando o comando “tracert 2001:db8:3:3::3”. O “traceroute”, invocado no *prompt do Windows* como “tracert” é uma ferramenta de diagnóstico que rastreia o caminho percorrido por um pacote IP registrando como “saltos” cada passagem por um roteador.

Como retorno o *prompt* informa que o pacote passou pelos roteadores 2, 3, 4 e 5 e suas respectivas redes. O objetivo era saber se o pacote teria atravessado as redes corretamente e como demonstrado, saltos registrados com sucesso.

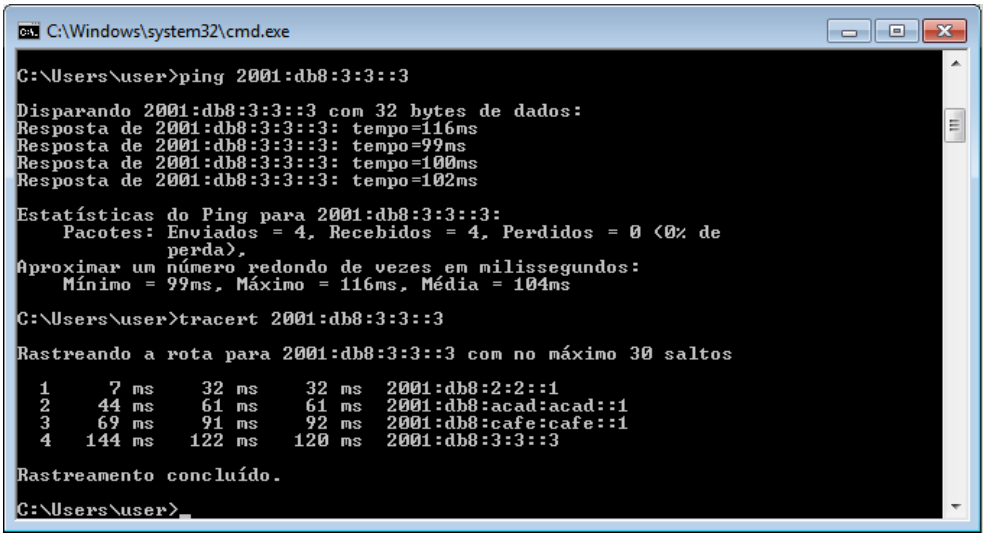

Figura 15: Ping e traceroute para o servidor Web.

Após a verificação de conectividade do servidor remoto, foi configurado na máquina virtual “W2008” o serviço DNS, com registros A e AAAA. Para esta simulação foram inseridos registros A do site **webtcc.internettcc** em IPv4 e o mesmo site com o registro AAAA, em IPv6. A intenção foi deixar ambos IPs para o mesmo site e deixar o *Happy Eyeballs* decidir qual conexão utilizar para este acesso.

Na Figura 16 é verificado a tabela DNS com os registros A (IPv4) e AAAA (IPv6) para o site “webtcc”.

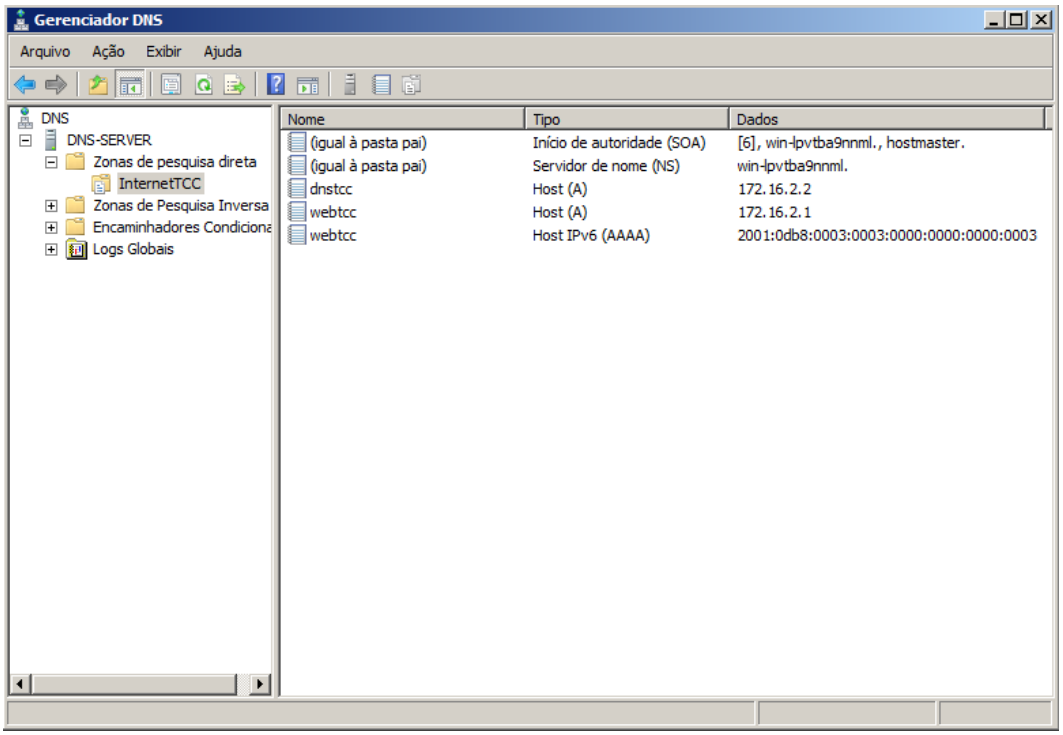

Figura 16: Tabela DNS e seus respectivos registros A e AAAA.

Para confirmar o uso do IPv6 na conexão com o site “webtcc.internettcc” em servidor-WEB, o tráfego foi capturado no enlace do servidor-WEB, utilizando o software “Wireshark”, que é um programa que analisa o tráfego de rede.

Como demonstrado nas Figuras 17 e 18, a conexão acontece exclusivamente em IPv6, devido a ação do *Happy Eyeballs*. Essa decisão de conexão é armazenada em um cache do cliente para a próxima tentativa de acesso (IPV6.BR, 2012).

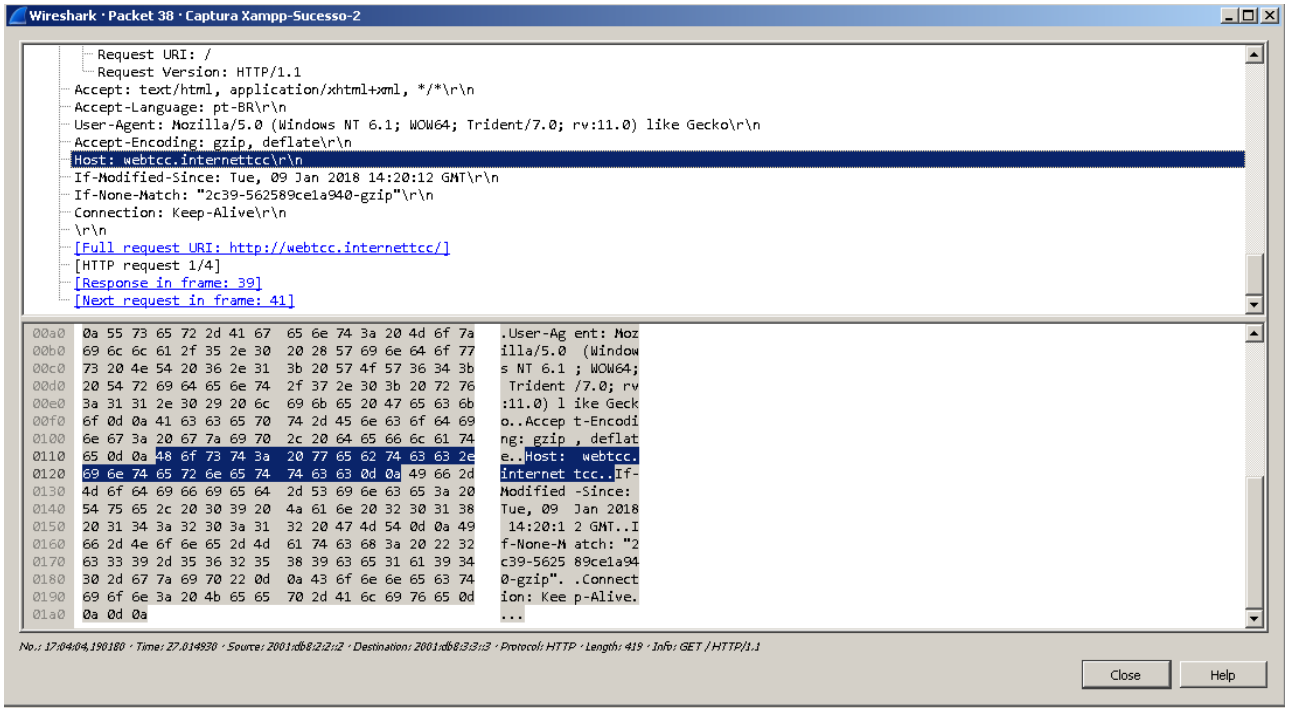

Figura 17: Captura de acesso ao servidor WEB no momento da requisição.

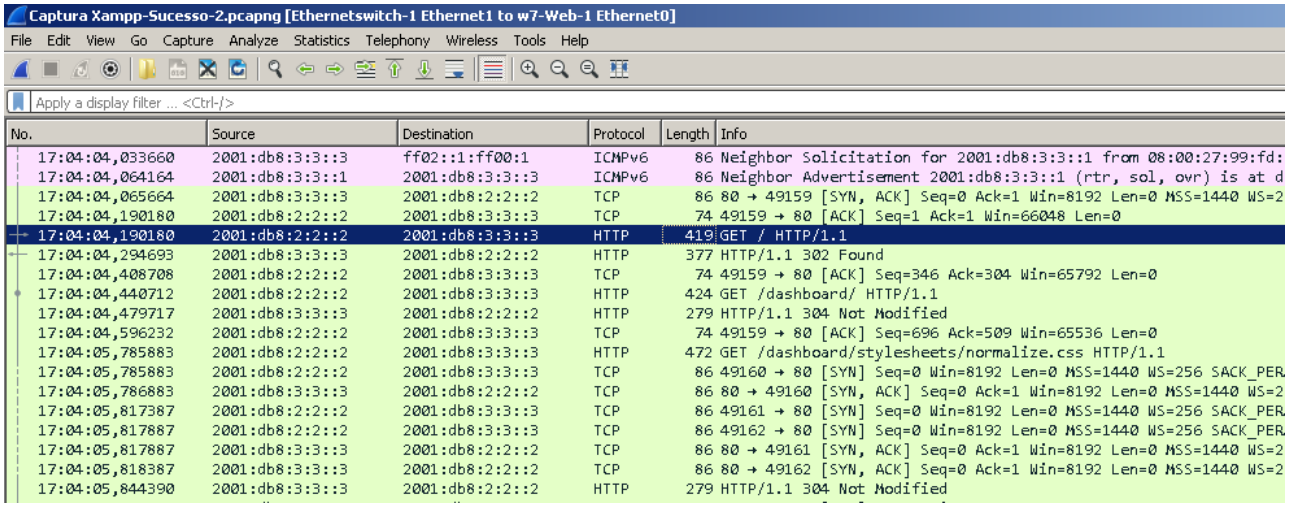

Figura 18: Acesso ao servidor web, captura de pacotes na conexão.

Ao decorrer do acesso, como resposta a requisição do site “webtcc.internettcc” o servidor DNS retorna o IPv6 para acesso http, como mostra a Figura 19.

O objetivo do acesso IPv6 em uma rede com Pilha Dupla foi alcançado, respeitando o fluxo normal de acesso a redes remotas. Foram configurados desde endereçamento pilha dupla em todas as interfaces ativas, inclusive o protocolo de roteamento entre as redes.

Com as informações desta simulação e a tabela de endereçamento IP (apêndice 1) se dá a condição básica para iniciar um processo de transição do IPv4 para o IPv6.

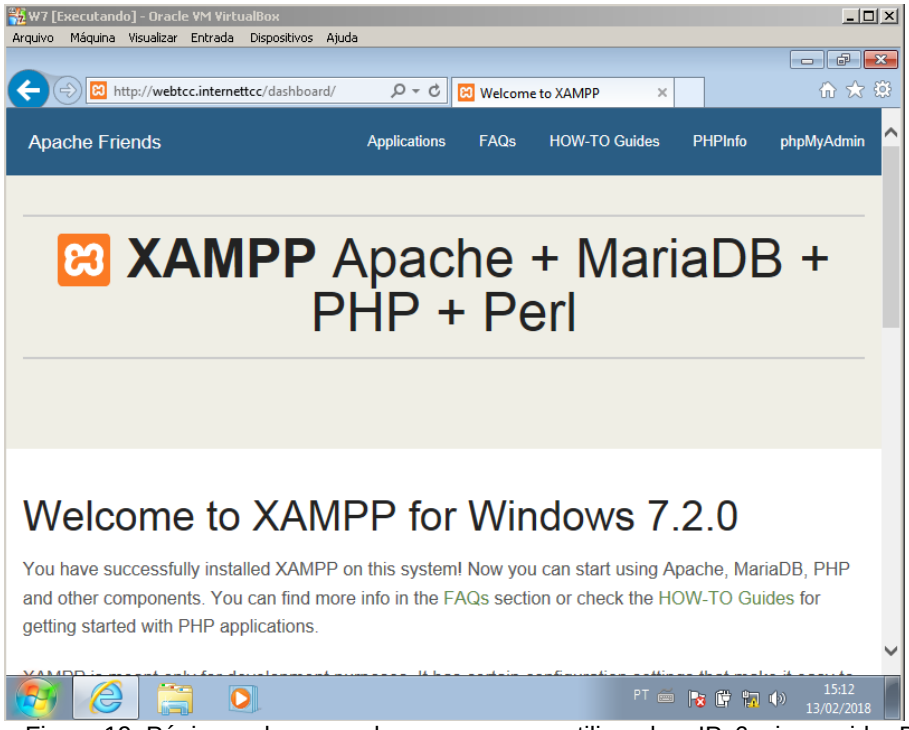

Figura 19: Página web acessada com sucesso, utilizando o IPv6, via servidor DNS.

7. CONSIDERAÇÕES FINAIS

A exaustão da oferta de endereços IPv4 trouxe preocupação para os órgãos reguladores da Internet e o advento de novas tecnologias colaborou mais ainda para a escassez de endereços IP versão 4.

Métodos paliativos para garantir sobrevida ao IPv4 como o CGNAT aumenta a preocupação com segurança e quebra o modelo de comunicação fim-a-fim da Internet. Comprometendo a versatilidade do serviço da Internet. O IPv6 vem para acabar com a escassez de IPs públicos.

Com seus 128 bits e possibilidade para conectar 340 undecilhões de hosts o IPv6 chegou para solucionar o problema de poupança de endereços IPs e está pronto para as novas tecnologias como a Internet das Coisas, que conecta casas, carros, dispositivos médicos e de vários fins para facilitar a vida do ser humano. Toda essa possibilidade abre nichos de mercado como inovação e segurança.

Mas os dois protocolos, o antigo versão 4 e o versão 6 não são compatíveis entre si. Foi uma decisão de projeto para ser assim e carece de uma transição. Foram desenvolvidas técnicas de tunelamento, tradução e pilha dupla, onde este último se configura os dois protocolos na mesma interface de rede. Este parece ser mais promissor pois deixa a estrutura empresarial ou residência pronta para uma iminente troca de protocolos.

Para o cenário empresarial é importante que as equipes tomem conhecimento do novo protocolo, que os desenvolvedores de aplicações tenham em vista que o suporte ao IPv6 não deve ser mais opcional e sim requisito básico para suas aplicações.

7.1. Em relação ao objetivo do trabalho

Para uma transição sem traumas é desejável que seja implementado a Pilha Dupla. Sua configuração inicial pode ser um pouco trabalhosa do ponto de vista de configuração pois precisa-se fazer um retrabalho endereçando interfaces e outras configurações já consolidadas.

Analisando do ponto de vista de benefícios, com certeza a adoção da Pilha Dupla infere em longo prazo melhores resultados. Aplicações legadas continuarão funcionando sem mais configurações para o futuro até gradativamente o IPv6 assumir a maioria do tráfego de dados da Internet.

Neste trabalho foi simulado, em um ambiente controlado, a conectividade em Pilha Dupla. Para qualquer tráfego, IPv4 ou IPv6 ou ambas, a rede está pronta para enviar e receber dados.

Num futuro provável, esta rede de computadores estará apta para o desligamento das conexões IPv4 sem mais configurações de interfaces de rede, salvo o provável movimento de crescimento da própria empresa e de sua infraestrutura.

7.2. Em relação aos objetivos específicos

No que tange custos de implantação, a pilha dupla se mostra promissora pois no limiar do final da década de 2010 a maioria dos dispositivos em operação têm compatibilidades com o IPv6.

Eventuais custos com aquisição de algum equipamento podem ser aceitáveis frente aos benefícios do IPv6. Não obstante a compra, deve-se considerar a atualização do sistema operacional de cada equipamento que normalmente é fornecida gratuitamente pelo fabricante.

Em relação à migração e implantação do IPv6, foram expostos em tópicos as melhores práticas para uma implementação segura, desde o endereçamento até a recomendação de uma empresa especializada para o trabalho.

Quanto ao resultado do experimento proposto, pode-se dizer que o objetivo foi alcançado uma vez que todos os dispositivos conectados naquela rede possuíam os dos protocolos IP, em cada interface, configurados. Foram executados testes de conectividade, demonstrados os alcances em servidor DNS e no servidor WEB, capturadas informações referentes a natureza dos dados trafegados e provado o tráfego IPv6 na pilha dupla, quando há disponibilidade na outra extremidade da comunicação IP.

7.3. Trabalhos futuros

Como trabalhos futuros e aprofundamento no assunto transição para o novo protocolo, é interessante verificar os serviços que rodam em 2º plano nos sistemas operacionais em geral relacionados à segurança.

Assim como no IPv4 que necessita de políticas de segurança como filtragem de pacotes, firewall, vulnerabilidades e acesso a informações; o IPv6 demanda dos mesmos cuidados, e num contexto de produção de pilha dupla, por exemplo, provoca 2 políticas de segurança distintas.

Aproveitando as atualizações de segurança que vieram nativamente no IPv6 (*Authentication Header* e *Encrypted Security Payload*) que trabalham na camada de rede, pode-se explorar as aplicações de segurança e implementação, principalmente em VPN´s onde a segurança é fundamental em redes dessa natureza onde transitam por redes públicas.

REFERÊNCIAS

BRITO, Samuel Henrique Bucke. **IPv6 - O novo protocolo da Internet.** São Paulo: Novatec, 2017. 208 p. E-book.

BRITO, Samuel Henrique Bucke. **Autoconfiguração de Endereços IPv6 (SLAAC).** 2013. Disponível em: <http://labcisco.blogspot.com.br/2013/05/autoconfiguracao-de-enderecos-ipv6-slaac.html> Acesso em: 13 out. 2017.

COMER, D. E. **Interligação de Redes com TCP/IP: princípios, protocolos e arquitetura**.5.ed. São Paulo: Elsevier, 2006.

COMER, D. E. **Redes de Computadores e Internet.** 4. ed. Porto Alegre: Bookman, 2007.

CIRIACO, Douglas. (Brasil). Tecmundo (Ed.). **O que é P2P?** 2008. Disponível em: <https://www.tecmundo.com.br/torrent/192-o-que-e-p2p-.htm>. Acesso em: 27 maio 2017.

CISCO (Estados Unidos). Cisco Networking Academy (Org.). **Curso CCNA 1 e 2.** 2014. Disponível em: <https://www.netacad.com/>. Acesso em: 15 abr. 2017.

DUMAS, Véronique. **A origem da internet.** 2013. Disponível em: <http://samuelmaia.blogspot.com.br/2013/07/a-origem-da-interne.html>. Acesso em: 05 jun. 2017.

EQUIPE IPV6.BR. 2012. **Transição**. Disponível em: <http://ipv6.br/entenda/transicao/>. Acesso em: 27 mai. 2017.

FRANCISCO, Wagner de Cerqueira e. **"A População Mundial"**; Brasil Escola. Disponível em <https://brasilescola.uol.com.br/geografia/populacao-mundial.htm>. Acesso em 14 mar. 2018.

GOMES, Alexandre José Camilo; TRINDADE, Carlos Botelho da. **Tutorial Rede IP.** 2012. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialredeipmig1/pagina_3.asp>. Acesso em: 16 maio 2017.

HAGEN, Silvia. **IPv6 Essentials.** 3. ed. Sebastopol: O’reilly Media, 2014. 412 p.

HUAWEI (China) (Org.). **IPv6 over IPv4.** 20--?. Disponível em: <http://support.huawei.com/enterprise/docinforeader!loadDocument1.action?contentId=DOC1000043927&partNo=10022>. Acesso em: 27 maio 2017.

KUROSE., J. F. ; ROSS, K. W. **Redes de Computadores e a Internet :Uma abordagem top- down** . 6.ed. São Paulo: Pearson, 2013.

LEVIN, Stanford L.; SCHMIDT, Stephen. **IPv4 to IPv6: Challenges, solutions, and lessons.** Telecommunications Policy, [s.l.], v. 38, n. 11, p.1059-1068, dez. 2014. Elsevier BV. http://dx.doi.org/10.1016/j.telpol.2014.06.008.

MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO; SECRETARIA DE LOGÍSTICA E TECNOLOGIA DA INFORMAÇÃO(Brasil). **Plano de Disseminação do Uso do IPv6.** Disponível em: http://www.governoeletronico.gov.br/biblioteca/arquivos/plano-de-disseminacao-do-uso-ipv6/view>. Acesso em: 10 mar. 2018

MOREIRAS, Antonio Marcos et al (Org.). **Apostila IPv6 Básico.** São Paulo: Nic.br, 2012. 154 p. Disponível em: <http://staff.on.br/mscorrea/IPv6/ApostilaIPv62012.pdf>. Acesso em: 15 abr. 2017.

Nic.br. Núcleo de Informação e Coordenação do Ponto Br (Org.). **Técnicas de Transição IPv6:** parte 02 (NAT444). 2014. Disponível em: <https://www.youtube.com/watch?v=dRIOPyf6Tx8>. Acesso em: 20 maio 2017.

REGISTRO DE ENDEREÇAMENTO DA INTERNET PARA A AMÉRICA LATINA - Portal LACNIC. **A única tecnologia possível para construir a Internet das Coisas é o IPv6.** 20--. Disponível em: <http://portalipv6.lacnic.net/pt-br/a-unica-tecnologia-possivel-para-construir-a-internet-das-coisas-e-o-ipv6/>. Acesso em: 23 mar. 2017.

RFC 1550. **IP: Next Generation (IPng) White Paper Solicitation**. 1993. Disponível em <https://www.ietf.org/rfc/rfc1550.txt>. Acesso em: 23 abr 2017.

RFC 2784. **Generic Routing Encapsulation (GRE)**. Disponível em: <https://www.ietf.org/rfc/rfc2784.txt>. Acesso em: 23 abr. 2017.

RFC 3022. **Traditional IP Network Address Translator (Traditional NAT).** 2001. Disponível em <https://www.ietf.org/rfc/rfc3022.txt> . Acesso em: 13 mai 2017.

RFC 6264. **An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition.** 2011. Disponível em <https://www.ietf.org/rfc/rfc6264.txt>. Acesso em: 21 dez 2017.

RFC 6555. **Happy Eyeballs: Success with Dual-Stack Hosts.** 2012. Disponível em <https://www.ietf.org/rfc/rfc6555.txt>. Acesso em: 12 fev 2018.

RFC 6598. **IANA-Reserved IPv4 Prefix for Shared Address Space**. Disponível em: <https://www.ietf.org/rfc/rfc6598.txt>. Acesso em: 27 abr. 2017.

SANTOS, Rodrigo Regis dos. **A importância do IPv6 para o futuro da Internet.** 2009. Disponível em: <http://www.ceptro.br/pub/CEPTRO/PalestrasPublicacoes/SELCOMP.pdf>. Acesso em: 14 abr. 2017.

TANENBAUM, A. S.; WETHERALL, D. J. **Redes de Computadores.** 5. ed. São Paulo: Elsevier, 2011.

WORLDOMETERS (Estados Unidos). Dadax (Comp.). **World Population.** 2017. Disponível em: <http://www.worldometers.info/>. Acesso em: 20 abr. 2017.

APÊNDICE 1

Tabela de endereçamento do experimento

Dispositivo	Local	Interface	IPv4	IPv6
Empresa-PC	Empresa	Fa0	192.168.2.1/24	2001:DB8:2:2::2/64
Router-Emp	Empresa	Fa0	192.168.2.254/24	2001:DB8:2:2::1/64
Router-Emp	Empresa	S0	200.120.123.2/24	2001:DB8:ACAD:ACAD::2/64
Router-ISP	ISP	S0	200.120.123.1/24	2001:DB8:ACAD:ACAD::1/64
Router-ISP	ISP	S1	200.120.122.2/24	2001:DB8:CAFE:CAFE::2/64
Router-Int	INTERNET	S0	200.120.122.1/24	2001:DB8:CAFE:CAFE::1/64
Router-Int	INTERNET	Fa0	172.16.2.254/24	2001:DB8:3:3::1/64
DNS	DNS	Fa0	172.16.2.2/24	2001:DB8:3:3::2/64
SERV-WEB	DNS	Fa0	172.16.2.1/24	2001:DB8:3:3::3/64

Configuração dos roteadores

Empresa

```
Current configuration : 1057 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router-Emp
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
```

```
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
ip tcp synwait-time 5
!
!
no ip domain lookup
!
ipv6 unicast-routing
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0
 ip address 192.168.2.254 255.255.255.0
 speed auto
 ipv6 address 2001:DB8:2:2::1/48
 ipv6 enable
```

```
 ipv6 rip TCC enable
!
interface Serial0
 ip address 200.120.123.2 255.255.255.0
 ipv6 address 2001:DB8:ACAD:ACAD::2/64
 ipv6 enable
 ipv6 rip TCC enable
!
router rip
 version 2
 network 192.168.2.0
 network 200.120.123.0
 no auto-summary
!
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
ipv6 router rip TCC
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
```

```
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
end
```

Router-ISP

```
Current configuration : 1113 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router-ISP
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
```

```
!
ip tcp synwait-time 5
!
!
no ip domain lookup
!
ipv6 unicast-routing
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0
 no ip address
 shutdown
 speed auto
!
interface Serial0
 ip address 200.120.123.1 255.255.255.0
 ipv6 address 2001:DB8:ACAD:ACAD::1/64
 ipv6 enable
```

```
 ipv6 rip TCC enable
!
interface Serial1
 ip address 200.120.122.2 255.255.255.0
 ipv6 address 2001:DB8:CAFE:CAFE::2/64
 ipv6 enable
 ipv6 rip TCC enable
!
router rip
 version 2
 network 200.120.122.0
 network 200.120.123.0
 no auto-summary
!
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
ipv6 router rip TCC
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
```

```
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
end
```

Router-Int

```
Current configuration : 1214 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router-Int
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
```

```
ip tcp synwait-time 5
!
!
no ip domain lookup
!
ipv6 unicast-routing
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0
 ip address 172.16.2.254 255.255.255.0
 speed auto
 ipv6 address 2001:DB8:3:3::1/64
 ipv6 enable
 ipv6 rip TCC enable
!
interface Serial0
 ip address 200.120.122.1 255.255.255.0
 ipv6 address 2001:DB8:CAFE:CAFE::1/64
```

```
 ipv6 enable
 ipv6 rip TCC enable
!
interface Serial1
 ip address 200.120.121.2 255.255.255.0
 ipv6 address 2001:DB8:CADE:CADE::2/64
 ipv6 enable
 ipv6 rip TCC enable
!
router rip
 version 2
 network 172.16.0.0
 network 200.120.121.0
 network 200.120.122.0
 no auto-summary
!
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
ipv6 router rip TCC
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
```

```
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
end
```